IBM Docket No. YOR920020159US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Applicants:	Date: July 15, 2004
Trapp et al.	Group Art Unit: 2152
Serial No.: 10/065,802	Examiner: Unknown
Filed: November 20, 2002	Docket No.: YOR920020159US1

For: **METHOD AND APPARATUS FOR SECURE PROCESSING OF SENSITIVE DATA**

Assistant Commissioner for Patents
Washington, D. C. 20231

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this paper (3 pages, Petition to make special) is being facsimile transmitted under Rule 37 CFR 1.6(d) to the U.S. Patent and Trademark Office to 703-306-5509 on July 15, 2004.

Derek S. Jennings
Registered Patent Agent / Senior Patent Agent
Reg. No. 41,473
Fax: 914-945-3281

REQUEST FOR RECONSIDERATION ON THE PETITION TO MAKE SPECIAL

UNDER 37 C.F.R. §1.102, MPEP 708.02 XI

INVENTIONS FOR COUNTERING TERRORISM

REMARKS

Applicants submit the following remarks on the request for reconsideration for the petition to make special the present patent application under 37 C.F.R. § 1.102 and MPEP 708.02 XI "Inventions for Countering Terrorism".

The present patent application can be used for countering terrorism. As mentioned in the MPEP, section 708.02 XI

> International terrorism as defined in 18 U.S.C. 2331 includes "activities that - (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; [and] (B) appear to be intended - (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by assassination or kidnapping..." The types of technology for countering terrorism could include, but are not limited to, systems for detecting/identifying explosives, aircraft sensors/security systems, and vehicular barricades/disabling systems.

and 35 U.S.C. § 1.102 "Advancement of examination" that states:

> (a) Applications will not be advanced out of turn for examination or for further action except as provided by this part, or upon order of the Commissioner to expedite the business of the Office, or upon filing of a request under paragraph (b) of this section or upon filing a petition under paragraphs (c) or (d) of this section with a showing which, in the opinion of the Commissioner, will justify so advancing it.
>
> (b) Applications wherein the inventions are deemed of peculiar importance to some branch of the public service and the head of some department of the Government requests immediate action for that reason, may be advanced for examination.
>
> (c) A petition to make an application special may be filed without a fee if the basis for the petition is the applicant's age or health or that the invention will materially enhance the quality of the environment or materially contribute to the development or conservation of energy resources.
>
> (d) A petition to make an application special on grounds other than those referred to in paragraph (c) of this section must be accompanied by the fee set forth in § 1.17(h).

Neither 37 CFR 102 nor MPEP 708.02 XI requires a petition to make special to base on the claimed invention. Applicants' patent application, as filed, reads on aspects for countering terrorism. Specifically, the following paragraphs highlight detail aspects to counter terrorism:

[0039]

For a screening scenario, the involved parties might be the service provider, who operates the screening service, the screener, who wants to check an individual, several information providers, which provide the watch list data, and parties like law enforcement, airport security or human resources, which should be informed in case the screened individual is found on a watch list.

[0040]

The information provider wants to keep his watch list data confidential, i.e. he allows its use for screening, but the information on the lists must not leak outside the system. The screener wants to guarantee basic privacy for the screened individuals as long as they do not show up on the watch lists. In particular, he does not want to enable the information provider to trace arbitrary individuals based on screening requests. Screener and information provider only want to notify law enforcement in case of a match and do not want to leak information in other cases. None of the parties wants that information leaks to the service provider or to intruders.

[0045]

The system allows different parties to interact at the same time based on different service specifications. For example, in a screening application, there can be a multitude of different screener parties, different information providers, and different law enforcement agencies. Each request sent to the system invokes processing based on a specified service specification. The service specification determines which parties interoperate in the processing of this request. For convenience, we also define composite contracts, see further below.

[0095]

Fig. 6 shows an example contract 601 for an application, where individuals are securely checked against watch lists according to an embodiment of the present invention. Fig. 6 gives an example for a contract, 601, that can be used to check individuals against watch lists of criminals. The information given in the table corresponds to the variables defined in the UML class diagrams in Figs. 3A and 3B. In this example, the contract identifier, 602, is "4711B5" and the involved parties, 603, which are named A, B, and C, are an airport, 603 A, which wants to screen applicants, a government agency, 603 B, which provides watch lists to be checked against, and a law enforcement office, 603 C, which should be notified, when a match is found.

[0100]

The first processing step is a 1:n Matching against a watch list named XYZ, 608. This processing step is owned by party B and is executed unconditionally (condition = True). The column named "1:n Matching"defines with +-signs the inputs for this processing step: first name, last name, and date of birth. Outputs are defined in the rows 608: a value stating whether the match was successful, first name, last name, date of birth, a suspect class, fingerprint data from file, information about previous convictions and reaction advice.

[0106] In a screening application, for example, this would allow a screener to have a contract for screening against watch lists from agency A and another contract for screening against watch lists from agency B. The combined contract would invoke both searches on behalf of a single request to the system. Other composite contracts may allow checking against yet other combinations.

[0107] Biometric information scanned at an entry point can be sent within a request to one or more servers, which process the data and can check it against multiple databases. The workflow is completely up to the participating parties, including sending an alarm to a law enforcement agency instead of returning data about the screened individual back to the screener.

[0115] Fig. 9 shows a screening scenario according to an embodiment of the present invention. The first one starts with a screening request 1110 from the screener 1101 to a server cell 1103. The cell 1103 receives the request through its network handler 1106 and passes it on into a coprocessor 1108 for processing. If the watch list that should be used for screening is available in this cell, the coprocessor 1108 queries the database 1109 for information about the individual. Then, it uses the network handler to notify law enforcement 1107. This notification is sent in any case. If there is no match, the notification contains a decoy, which is not displayed as an alarm at law enforcement. After the law enforcement 1107 acknowledgement is received, the screener 1101 is notified that his request was processed.

It is well known that the Department of Homeland Security (DHS) issues directives controlling the nation's airports and rail systems. Recent DHS directives include:

Travel Security

U.S. and EU Agreement on Passenger Data

On May 11, 2004, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) issued the document set forth below (the "Undertakings[1]"). These Undertakings contain a set of representations regarding the manner in which CBP will handle certain Passenger Name Record (PNR) data relating to flights between the United States and EU member states, access to which is required under U.S. law (49 U.S.C. 44909).

These Undertakings provide the framework within which the European Union (EU) was able to approve several measures which the EU requires to permit the transfer of such PNR data to CBP, consistent with EU law. On May 17, 2004, the European Commission announced that it had issued an "adequacy finding" decision for the transfer of such PNR

[1] See attachment 1 for the entire "Undertaking.

data to CBP, and a related international agreement was also approved by the European Council for execution on May 28, 2004

Travel Security

Fact Sheet: CAPPS II at a Glance

For Immediate Release
Press Office
Contact: 202-282-8010
February 12, 2004

What is CAPPS II?

The enhanced Computer Assisted Passenger Prescreening System (CAPPS II) is a limited, automated prescreening system authorized by Congress in the wake of the Sept. 11, 2001 terrorist attacks. The system, developed with the utmost concern for individual privacy rights, modernizes the prescreening system currently implemented by the airlines. **It will seek to authenticate travelers' identities and perform risk assessments to detect individuals who may pose a terrorist-related threat or who have outstanding Federal or state warrants for crimes of violence.**

....

Under CAPPS II, airlines will ask passengers for a slightly expanded amount of reservation information, including full name, date of birth, home address, and home telephone number. With this expanded information, the system will quickly verify the identity of the passenger and conduct a risk assessment utilizing commercially available data and current intelligence information. The risk assessment will result in a recommended screening level, categorized as no risk, unknown or elevated risk, or high risk. The commercially available data will not be viewed by government employees, and intelligence information will remain behind the government firewall. The entire prescreening process is expected to take as little as five seconds to complete.

Once the system has computed a traveler's risk score, it will send an encoded message to be printed on the boarding pass indicating the appropriate level of screening. Eventually, the information relevant to the appropriate screening process is planned to be transmitted directly to screeners at security checkpoints.

In the rare instances where a particular traveler has been identified as having known or suspected links to terrorism or has an outstanding Federal or state warrant for a crime of violence, appropriate law enforcement officers will be notified. A small percentage of passengers will require additional screening at the security checkpoint. The vast majority of travelers will go through the normal screening process.

....

How will CAPPS II strengthen homeland security?
A vital element of TSA's layered approach to security is to ensure that travelers who are known or potential threats to aviation are stopped before they or their baggage board an aircraft. CAPPS II is an integral part of that approach. It provides:

- A stronger prevention system - CAPPS II will provide a more reliable screening result than is provided by the current airline operated prescreening system. It will seek to authenticate a passenger's identity and conduct a risk assessment. It also allows for updates as new intelligence is received and the threat level is modified.
- Shorter waits at checkpoints -- By reducing the number of selectees requiring additional screening, CAPPS II will help speed up the screening process for the vast majority of travelers.
- Focus for resources -- CAPPS II will enable DHS to focus its screening resources and as DHS is better able to assess the potential risks to passengers and aircraft, it will be able to allocate resources such as the Federal Air Marshals.

Specifically, one embodiment of the present invention uses a screening scenario that includes a screener who wants to check an individual against information, a watch list, provided by several information providers. Parties like law enforcement and airport security can be informed in case the screened individual is found to be on the watch list.

The present patent application is further directed for countering terrorism as embodiment in applicants' original claim 33 and previously presented claims 37, 55 – 58 and 65 – 68[2].

The Special Program Examiner mistakenly stated that the present patent application does not monitor for terrorists or potential terrorist acts. The present patent application clearly provides notification to the police departments, airport security and/or government agencies for individuals that may be on a "watch list".

The present invention protects the nation against further terrorist attacks by allowing government agencies, airlines, rail and bus transportation systems, and private companies to analyze terrorism threats thereby protecting our critical infrastructure and

[2] See attachment 2.

the American way of life. Accordingly, applicants' petition to make special should be GRANTED and the patent application should be forwarded for immediate examination on the merits.

Please charge the petition fee under 37 CFR 1.17(h) or any other fee necessary to enter this paper and any previous paper to deposit account 09-0468.

Respectfully submitted,

By: ______________________________
Derek S. Jennings
Registered Patent Agent
Senior Patent Agent
Reg. No. 41,473

IBM Corporation
Intellectual Property Law Department
P. O. Box 218
Yorktown Heights, New York 10598
Telephone No.: (914) 945-2144

Attachment 1

UNDERTAKINGS OF THE DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP)

In support of the plan of the European Commission (Commission) to exercise the powers conferred on it by Article 25(6) of Directive 95/46/EC (the Directive) and to adopt a decision recognizing the Department of Homeland Security Bureau of Customs and Border Protection (CBP) as providing adequate protection for the purposes of air carrier transfers of Passenger[1] Name Record (PNR) data which may fall within the scope of the Directive, CBP undertakes as follows:

Legal Authority to Obtain PNR

1) By legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide CBP (formerly, the U.S. Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems");

Use of PNR Data by CBP

2) Most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically will significantly enhance CBP's ability to facilitate *bona fide* travel and conduct efficient and effective advance risk assessment of passengers;

3) PNR data is used by CBP strictly for purposes of preventing and combating: 1) terrorism and related crimes; 2) other serious crimes, including organized crime, that are transnational in nature; and 3) flight from warrants or custody for the crimes described above. Use of PNR data for these purposes permits CBP to focus its resources on high risk concerns, thereby facilitating and safeguarding *bona fide* travel;

Data Requirements

4) Data elements which CBP requires are listed herein at Attachment "A". (Such identified elements are hereinafter referred to as "PNR" for purposes of these Undertakings). Although CBP requires access to each of those thirty-four (34) data elements listed in Attachment "A", CBP believes that it will be rare that an individual PNR will include a full set of the identified data. In those instances where the PNR does not include a full set of the identified data, CBP will not seek direct access from the air carrier's reservation system to other PNR data which are not listed on Attachment "A";

5) With respect to the data elements identified as "OSI" and "SSI/SSR" (commonly referred to as general remarks and open fields), CBP's automated system will search those fields for any of the other data elements identified in Attachment "A". CBP personnel will not be authorized to manually review the full OSI and SSI/SSR fields

[1] For the purposes of these Undertakings, the terms "passenger" and "passengers" shall include crew members.

unless the individual that is the subject of a PNR has been identified by CBP as high risk in relation to any of the purposes identified in paragraph 3 hereof;

6) Additional personal information sought as a direct result of PNR data will be obtained from sources outside the government only through lawful channels, including through the use of mutual legal assistance channels where appropriate, and only for the purposes set forth in paragraph 3 hereof. For example, if a credit card number is listed in a PNR, transaction information linked to that account may be sought, pursuant to lawful process, such as a subpoena issued by a grand jury or a court order, or as otherwise authorized by law. In addition, access to records related to e-mail accounts derived from a PNR will follow U.S. statutory requirements for subpoenas, court orders, warrants, and other processes as authorized by law, depending on the type of information being sought;

7) CBP will consult with the European Commission regarding revision of the required PNR data elements (Attachment "A"), prior to effecting any such revision, if CBP becomes aware of additional PNR fields that airlines may add to their systems which would significantly enhance CBP's ability to conduct passenger risk assessments or if circumstances indicate that a previously non-required PNR field will be needed to fulfill the limited purposes referred to in paragraph 3 of these Undertakings;

8) CBP may transfer PNRs on a bulk basis to the Transportation Security Administration (TSA) for purposes of TSA's testing of its Computer Assisted Passenger Prescreening System II (CAPPS II). Such transfers will not be made until PNR data from US domestic flights has first been authorized for testing. PNR data transferred under this provision will not be retained by TSA or any other parties directly involved in the tests beyond the period necessary for testing purposes, or be transferred to any other third party[2]. The purpose of the processing is strictly limited to testing the CAPPS II system and interfaces, and, except in emergency situations involving the positive identification of a known terrorist or individual with established connections to terrorism, is not to have any operational consequences. Under the provision requiring an automated filtering method described in paragraph 10, CBP will have filtered and deleted "sensitive" data before transferring any PNRs to TSA on a bulk basis under this paragraph

Treatment of "Sensitive" Data

9) CBP will not use "sensitive" data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning the health or sex life of the individual) from the PNR, as described below;

10) CBP will implement, with the least possible delay, an automated system which filters and deletes certain "sensitive" PNR codes and terms which CBP has identified in consultation with the European Commission;

11) Until such automated filters can be implemented CBP represents that it does not and will not use "sensitive" PNR data and will undertake to delete "sensitive" data from any discretionary disclosure of PNR under paragraphs 28-34;[3]

[2] For purposes of this provision, CBP is not considered a party directly involved in the CAPPS II testing or a "third party."

[3] Prior to CBP's implementation of automated filters (as referenced in paragraph 10 hereof), if "sensitive" data exists in a PNR which is the subject of a non-discretionary disclosure by CBP as described in

Method of Accessing PNR Data

12) With regard to the PNR data which CBP accesses (or receives) directly from the air carrier's reservation systems for purposes of identifying potential subjects for border examination, CBP personnel will only access (or receive) and use PNR data concerning persons whose travel includes a flight into or out of[4] the United States;

13) CBP will "pull" passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to "push" the data to CBP;

14) CBP will pull PNR data associated with a particular flight no earlier than 72 hours prior to the departure of that flight, and will re-check the systems no more than three (3) times between the initial pull, the departure of the flight from a foreign point and the flight's arrival in the United States, or between the initial pull and the departure of the flight from the United States, as applicable, to identify any changes in the information. In the event that the air carriers obtain the ability to "push" PNR data, CBP will need to receive the data 72 hours prior to departure of the flight, provided that all changes to the PNR data which are made between that point and the time of the flight's arrival in or departure from the U.S., are also pushed to CBP.[5] In the unusual event that CBP obtains advance information that person(s) of specific concern may be travelling on a flight to, from or through the U.S., CBP may pull (or request a particular push) of PNR data prior to 72 hours before departure of the flight to ensure proper enforcement action may be taken when essential to prevent or combat an offense enumerated in paragraph 3 hereof. To the extent practicable, in such instances where PNR data must be accessed by CBP prior to 72 hours before the departure of the flight, CBP will utilize customary law enforcement channels;

Storage of PNR Data

15) Subject to the approval of the National Archives and Records Administration (44 U.S.C. 2101, et seq.), CBP will limit on-line access to PNR data to authorized CBP users[6] for a period of seven (7) days, after which the number of officers authorized to access the PNR data will be even further limited for a period of three years and 6 months (3.5 years) from the date the data is accessed (or received) from the air carrier's reservation system. After 3.5 years, PNR data that has not been manually accessed during that period of time, will be destroyed. PNR data that has been manually accessed during the initial 3.5 year period will be transferred by CBP to a deleted record file,[7]

paragraph 35 hereof, CBP will make every effort to limit the release of "sensitive" PNR data, consistent with U.S. law.

[4] This would include persons transiting through the United States.

[5] In the event that the air carriers agree to push the PNR data to CBP, the agency will engage in discussions with the air carriers regarding the possibility of pushing PNR data at periodic intervals between 72 hours before departure of the flight from a foreign point and the flight's arrival in the United States, or within 72 hours before the departure of the flight from the United States, as applicable. CBP seeks to utilize a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment, while minimizing the economic impact upon air carriers.

[6] These authorized CBP users would include employees assigned to analytical units in the field offices, as well as employees assigned to the National Targeting Center. As indicated previously, persons charged with maintaining, developing or auditing the CBP database will also have access to such data for those limited purposes.

[7] Although the PNR record is not technically deleted when it is transferred to the Deleted Record File, it is stored as raw data (not a readily searchable form and, therefore, of no use for "traditional" law enforcement investigations) and is only available to authorized personnel in the Office of Internal Affairs for CBP (and

where it will remain for a period of eight (8) years before it is destroyed. This schedule, however, would not apply to PNR data that is linked to a specific enforcement record (such data would remain accessible until the enforcement record is archived). With respect to PNR which CBP accesses (or receives) directly from air carrier reservation systems during the effective dates of these Undertakings, CBP will abide by the retention policies set forth in the present paragraph, notwithstanding the possible expiration of the Undertakings pursuant to paragraph 46 herein;

CBP Computer System Security

16) Authorized CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the Customs Data Center. PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system;

17) No other foreign, federal, state or local agency has direct electronic access to PNR data through CBP databases (including through the Interagency Border Inspection System (IBIS));

18) Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system;

19) Only certain CBP officers, employees or information technology contractors[8] (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data;

20) CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements;

21) Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR is subject to strict disciplinary action (which may include termination of employment) and may result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030);

22) CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34);

in some cases the Office of the Inspector General in connection with audits) and personnel responsible for maintaining the database in CBP's Office of Information Technology, on a "need to know" basis.

[8] Access by "contractors" to any PNR data contained in the CBP computer systems would be confined to persons under contract with CBP to assist in the maintenance or development of CBP's computer system.

23) Criminal penalties (including fines, imprisonment of up to one year, or both) may be assessed against any officer or employee of the United States for disclosing PNR data obtained in the course of his employment, where such disclosure is not authorized by law (see title 18, United States Code, sections 641, 1030, 1905);

CBP Treatment and Protection of PNR Data

24) CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as in accordance with these Undertakings or as otherwise required by law;

25) Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA. Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure where the information is confidential commercial information, where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy, or where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy (title 5, United States Code, sections 552(b)(4), (6), (7)(C));

26) CBP regulations (title 19, Code of Federal Regulations, section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to: (1) confidential commercial information; (2) material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and (3) information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy.[9]

27) CBP will take the position in connection with any administrative or judicial proceeding arising out of a FOIA request for PNR information accessed from air carriers, that such records are exempt from disclosure under the FOIA;

Transfer of PNR Data to Other Government Authorities

28) With the exception of transfers between CBP and TSA pursuant to paragraph 8 herein, Department of Homeland Security (DHS) components will be treated as "third agencies", subject to the same rules and conditions for sharing of PNR data as other government authorities outside DHS;

29) CBP, in its discretion, will only provide PNR data to other government authorities, including foreign government authorities, with counter-terrorism or law enforcement functions, on a case-by-case basis, for purposes of preventing and combating offenses

[9] CBP would invoke these exemptions uniformly, without regard to the nationality or country of residence of the subject of the data.

identified in paragraph 3 herein. (Authorities with whom CBP may share such data shall hereinafter be referred to as the "Designated Authorities");

30) CBP will judiciously exercise its discretion to transfer PNR data for the stated purposes. CBP will first determine if the reason for disclosing the PNR data to another Designated Authority fits within the stated purpose (see paragraph 29 herein). If so, CBP will determine whether that Designated Authority is responsible for preventing, investigating or prosecuting the violations of, or enforcing or implementing, a statute or regulation related to that purpose, where CBP is aware of an indication of a violation or potential violation of law. The merits of disclosure will need to be reviewed in light of all the circumstances presented;

31) For purposes of regulating the dissemination of PNR data which may be shared with other Designated Authorities, CBP is considered the "owner" of the data and such Designated Authorities are obligated by the express terms of disclosure to: (1) use the PNR data only for the purposes set forth in paragraph 29 or 34 herein, as applicable; (2) ensure the orderly disposal of PNR information that has been received, consistent with the Designated Authority's record retention procedures; and (3) obtain CBP's express authorization for any further dissemination. Failure to respect the conditions for transfer may be investigated and reported by the DHS Chief Privacy Officer and may make the Designated Authority ineligible to receive subsequent transfers of PNR data from CBP;

32) Each disclosure of PNR data by CBP will be conditioned upon the receiving agency's treatment of this data as confidential commercial information and law enforcement sensitive, confidential personal information of the data subject, as identified in paragraphs 25 and 26 hereof, which should be treated as exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552). Further, the recipient agency will be advised that further disclosure of such information is not permitted without the express prior approval of CBP. CBP will not authorize any further transfer of PNR data for purposes other than those identified in paragraphs 29, 34 or 35 herein;

33) Persons employed by such Designated Authorities who without appropriate authorization disclose PNR data, may be liable for criminal sanctions (title 18, United States Code, sections 641, 1030, 1905);

34) No statement herein shall impede the use or disclosure of PNR data to relevant government authorities, where such disclosure is necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks. Disclosures for these purposes will be subject to the same conditions for transfers set forth in paragraphs 31 and 32 of these Undertakings;

35) No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings;

Notice, Access and Opportunities for Redress for PNR Data Subjects

36) CBP will provide information to the traveling public regarding the PNR requirement and the issues associated with its use (i.e., general information regarding the authority under which the data is collected, the purpose for the collection, protection of the data, data sharing, the identity of the responsible official, procedures available for

redress and contact information for persons with questions or concerns, etc., for posting on CBP's website, in travel pamphlets, etc.);

37) Requests by the data subject (also known as "first party requesters") to receive a copy of PNR data contained in CBP databases regarding the data subject are processed under the Freedom of Information Act (FOIA). Such requests may be addressed to: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229, if by mail; or such request may be delivered to the Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters, Washington, D.C. For further information regarding the procedures for making FOIA requests are contained in section 103.5 of title 19 of the U.S. Code of Federal Regulations. In the case of a first-party request, the fact that CBP otherwise considers PNR data to be confidential personal information of the data subject and confidential commercial information of the air carrier will not be used by CBP as a basis under FOIA for withholding PNR data from the data subject;

38) In certain exceptional circumstances, CBP may exercise its authority under FOIA to deny or postpone disclosure of all (or, more likely, part) of the PNR record to a first party requester, pursuant to title 5, United States Code, section 552(b) (e.g., if disclosure under FOIA "could reasonably be expected to interfere with enforcement proceedings" or "would disclose techniques and procedures for law enforcement investigations...[which] could reasonably be expected to risk circumvention of the law"). Under FOIA, any requester has the authority to administratively and judicially challenge CBP's decision to withhold information (see 5 U.S.C. 552(a)(4)(B); 19 CFR 103.7-103.9);

39) CBP will undertake to rectify[10] data at the request of passengers and crewmembers, air carriers or Data Protection Authorities (DPAs) in the EU Member States (to the extent specifically authorized by the data subject), where CBP determines that such data is contained in its database and a correction is justified and properly supported. CBP will inform any Designated Authority which has received such PNR data of any material rectification of that PNR data;

40) Requests for rectification of PNR data contained in CBP's database and complaints by individuals about CBP's handling of their PNR data may be made, either directly or via the relevant DPA (to the extent specifically authorized by the data subject) to the Assistant Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229;

41) In the event that a complaint cannot be resolved by CBP, the complaint may be directed, in writing, to the Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, who will review the situation and endeavor to resolve the complaint;[11]

[10] By "rectify", CBP wishes to make clear that it will not be authorized to revise the data within the PNR record that it accesses from the air carriers. Rather, a separate record linked to the PNR record will be created to note that the data was determined to be inaccurate and the proper correction. Specifically, CBP will annotate the passenger's secondary examination record to reflect that certain data in the PNR may be or is inaccurate.

[11] The DHS Chief Privacy Officer is independent of any directorate within the Department of Homeland Security. She is statutorily obligated to ensure that personal information is used in a manner than complies with relevant laws (see footnote 13). The determinations of the Chief Privacy Officer shall be binding on the Department and may not be overturned on political grounds.

42) Additionally, the DHS Privacy Office will address on an expedited basis complaints referred to it by DPAs in the European Union (EU) Member States on behalf of an EU resident to the extent such resident has authorized the DPA to act on his or her behalf and believes that his or her data protection complaint regarding PNR has not been satisfactorily dealt with by CBP (as set out in paragraphs 37-41 of these Undertakings) or the DHS Privacy Office. The Privacy Office will report its conclusions and advise the DPA or DPAs concerned regarding actions taken, if any. The DHS Chief Privacy Officer will include in her report to Congress issues regarding the number, the substance and the resolution of complaints regarding the handling of personal data, such as PNR;[12]

Compliance Issues

43) CBP, in conjunction with DHS, undertakes to conduct once a year, or more often if agreed by the parties, a joint review with the European Commission assisted as appropriate by representatives of European law enforcement authorities and/or authorities of the Member States of the European Union,[13] on the implementation of these Undertakings, with a view to mutually contributing to the effective operation of the processes described in these Undertakings;

44) CBP will issue regulations, directives or other policy documents incorporating the statements herein, to ensure compliance with these Undertakings by CBP officers, employees and contractors. As indicated herein, failure of CBP officers, employees and contractors to abide by CBP's policies incorporated therein may result in strict disciplinary measures being taken, and criminal sanctions, as applicable;

Reciprocity

45) In the event that an airline passenger identification system is implemented in the European Union which requires air carriers to provide authorities with access to PNR data for persons whose current travel itinerary includes a flight to or from the European Union, CBP shall, strictly on the basis of reciprocity, encourage U.S.-based airlines to cooperate;

[12] Pursuant to section 222 of the Homeland Security Act of 2002 (the "Act") (Public Law 107-296, dated November 25, 2002), the Privacy Officer for DHS is charged with conducting a "privacy impact assessment" of proposed rules of the Department on "on the privacy of personal information, including the type of personal information collected and the number of people affected" and must report to Congress on an annual basis regarding the "activities of the Department that affect privacy...." Section 222(5) of the Act also expressly directs the DHS Privacy Officer to hear and report to Congress regarding all "complaints of privacy violations."

[13] The composition of the teams on both sides will be notified to each other in advance and may include appropriate authorities concerned with privacy/data protection, customs control and other forms of law enforcement, border security and/or aviation security. Participating authorities will be required to obtain any necessary security clearances and will adhere to the confidentiality of the discussions and documentation to which they may be given access. Confidentiality will not however be an obstacle to each side making an appropriate report on the results of the joint review to their respective competent authorities, including the US Congress and the European Parliament. However, under no circumstances may participating authorities disclose any personal data of a data subject; nor may participating authorities disclose any non-public information derived from documents to which they are given access, or any operational or internal agency information they obtain during the joint review. The two sides will mutually determine the detailed modalities of the joint review.

Review and Termination of Undertakings

46) These Undertakings shall apply for a term of three years and six months (3.5 years), beginning on the date upon which an agreement enters into force between the United States and the European Community, authorizing the processing of PNR data by air carriers for purposes of transferring such data to CBP, in accordance with the Directive. After these Undertakings have been in effect for two years and six months (2.5 years), CBP, in conjunction with DHS, will initiate discussions with the Commission with the goal of extending the Undertakings and any supporting arrangements, upon mutually acceptable terms. If no mutually acceptable arrangement can be concluded prior to the expiration date of these Undertakings, the Undertakings will cease to be in effect;

No Private Right or Precedent Created

47) These Undertakings do not create or confer any right or benefit on any person or party, private or public.

48) The provisions of these Undertakings shall not constitute a precedent for any future discussions with the European Commission, the European Union, any related entity, or any third State regarding the transfer of any form of data.

May 11, 2004

Attachment "A"

PNR Data Elements Required by CBP from Air Carriers

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address(es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/Divided PNR information
17. Email address
18. Ticketing field information
19. General remarks
20. Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information
27. SSI/SSR information
28. Received from information
29. All historical changes to the PNR
30. Number of travelers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS information
34. ATFQ fields

Attachment 2

Partial listing of the Claims

33. An identification apparatus for matching individuals, the apparatus comprising: at least one host computer adapted to have at least one secure co-processor operating in a secure computation environment, said at least one host computer operative to: negotiate a machine interpretable contract between all parties, which would cooperate with a particular application running on said host computer; upload said contract into said secure computation environment; enforce said contract with regards to all cooperating parties; receive a service request from a requestor; execute secure processing of said service request; and provide notifications as defined in the contract.

37. An identification method for matching individuals, the method comprising the steps of:
providing at least one host computer adapted to have at least one secure co-processor operating in a secure computation environment;
operating said at least one host computer to negotiate a machine interpretable contract between all parties, which would cooperate with a particular application running on said host computer;
uploading said contract into said secure computation environment;
enforcing said contract with regards to all cooperating parties;
receiving a service request from a requestor;
executing secure processing of said service request; and
providing notifications as defined in the contract.

55. A computer-based method for managing a matching identification service, the method comprising the steps of:

implementing on a computer system at least one contract having a contract ID for governing said matching identification service between a service provider, a client and at least one other party determining, in accordance with said contract ID, whether a match exists between a first request from said client and a data response from one of at least one other party;

if a match results from said determining step, providing a notification of said match to said at least one other party.

56. The method of claim 55 further comprises the step of providing said notification even if there is no match as determined in said determining step.

57. The method of claim 56, wherein said step of providing said notification comprises the step of providing a dummy message to said at least one other party.

58. The method of claim 55 further comprises the step of notifying said client that said first request was processed.

65. Apparatus for a matching identification service, the apparatus comprising:

at least one host computer operative to: maintain and enforce at least one contract having a contract ID for governing a service between a service provider, a client and at least one other party; and to determine, in accordance with said at least one contract, whether a match exists between a first request from said client and a data response from one of at least one other party;

said at least one host computer is further operative to provide a notification to said at least one other party if a match results from said determination.

66. The apparatus of claim 65, wherein said at least one host computer comprises:

a secure computation environment for processing sensitive data;

a network handler for sending and receiving messages to and from said secure computation environment and a network; and a storage handler to process database requests that come from inside said secure computation environment and retrieves information from a secured database containing said contracts and private information data.

67. The apparatus of claim 66, wherein said secure computation environment comprises a contract engine operative to: handle said first request, conduct a matching task, and provide a respond serving as said notification.

68. The apparatus of claim 65, wherein said at least one host computer is further operative to provide said notification to said at least one other party if no match results from said determination.